Mark C. Mao, CA Bar No. 236165
Beko Reblitz-Richardson, CA Bar No. 238027
Alexander J. Konik, CA Bar No. 299291
BOIES SCHILLER FLEXNER LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
Fax: (415) 293-6899
mmao@bsfllp.com
brichardson@bsfllp.com
akonik@bsfllp.com

James Lee (*pro hac* admission pending)
Rossana Baeza (*pro hac* admission pending)
BOIES SCHILLER FLEXNER LLP
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
Fax: (303) 539-1307
jlee@bsfllp.com
rbaeza@bsfllp.com

Jesse Panuccio (*pro hac* admission pending)
BOIES SCHILLER FLEXNER LLP
1401 New York Ave, NW
Washington, DC 20005
Tel.: (202) 237-2727
Fax: (202) 237-6131
jpanuccio@bsfllp.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ and JULIEANNA MUNIZ individually and on behalf of all other similarly situated,

Plaintiffs,

v.

GOOGLE LLC and ALPHABET INC.,

Defendants.

Case No. 3:20-cv-4688

COMPLAINT

CLASS ACTION FOR
(1) FEDERAL WIRETAP VIOLATIONS, 18 U.S.C. §§ 2510, *ET. SEQ.*;
(2) INVASION OF PRIVACY ACT VIOLATIONS, CAL. PENAL CODE §§ 631 & 632;
(3) INVASION OF PRIVACY;
(4) COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT, CAL. PENAL CODE § 502.

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

This action arises from the unlawful and intentional interception and collection of individuals' confidential communications and data without their knowledge or consent, even when those individuals expressly follow the recommendations of defendants Google LLC and its parent company Alphabet Inc. (collectively, "Google" or "Defendants") to prevent the interception or collection of their browsing and other activity on their mobile apps. Plaintiffs Anibal Rodriguez and JulieAnna Muniz, individually and on behalf of all others similarly situated, file this class action against Google, and in support state the following:

I. INTRODUCTION

1. Google promises user control and privacy. In reality, Google is a voyeur extraordinaire. Google is always watching. Even when it promises to look away, Google is watching. Every click, every website, every app—our entire virtual lives. Intercepted. Tracked. Logged. Compiled. Packaged. Sold for profit.

2. This case is about Google's illegal interception of consumers' private activity on consumer mobile applications ("apps")—a huge and growing treasure trove of data that Google amasses by the second to sustain profits in its ever-growing share of the market for consumer advertising.

3. Protecting data privacy is critical in our increasingly virtual and interconnected society. People everywhere are becoming more aware and more concerned, that large corporations are intercepting, collecting, recording and exploiting for profit their personal communications and private information.

4. Well aware of these justified and growing concerns over privacy, Google—one of the world's largest technology companies—has assured and continues to assure its consumers and users that when it comes to mobile app activity, they and not Google, are "in control of what information [they] share with Google." For example, Google's global Privacy Policy states on the first page:

> When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and ***put you in control***.

> …
> Our services include: … ***products that are integrated into third-party apps*** and sites, like ads and embedded Google Maps.
> …
> ***[A]cross our services, you can adjust your privacy settings to control what we collect*** and how your information is used.

(emphasis added).

5. Google purports to offer consumers the option to "control" what app browsing and activity data Google collects by adjusting their privacy settings to "turn Web & App Activity off . . . at any time" before opening or browsing mobile apps. Google repeatedly assures its consumers that they need only "[t]urn Web & App Activity on or off" to control what app activity Google can and cannot see.

6. Google's privacy promises and assurances are blatant lies.

7. Google in fact intercepts, tracks, collects and sells consumer mobile app browsing history and activity data ***regardless of what*** safeguards or "privacy settings" consumers undertake to protect their privacy. Even when consumers follow Google's own instructions and turn off "Web & App Activity" tracking on their "Privacy Controls," Google nevertheless continues to intercept consumers' app usage and app browsing communications and personal information. Indeed, even if consumers completely avoid using Google-branded apps and devices, Google still tracks and compiles their communications by covertly integrating Google's tracking software into the products of other companies. Google's illegal practices extend to hundreds of thousands of smartphone apps, such as apps for The New York Times, Lyft, Alibaba, The Economist and others.

8. Google accomplishes this surreptitious and unlawful interception, tracking, and data collection of users' app activity through its Firebase SDK (software development kits). Firebase SDK is a suite of software tools that purports to provide additional functionality to an app, especially if it is to be released for Android. Third-party apps use Firebase SDK because its implementation is a prerequisite before Google allows access to its other tools such as Google Analytics, use of Google's ad exchanges (such as AdMob, explained below), and marketing of those apps on the Google Play Store. Developers often have no choice but to use Firebase SDK because of Google's demands and market power, including with analytics, advertisements, and the Android mobile

operating system. Once third-party app developers implement Firebase SDK, however, Firebase SDK allows Google to automatically and systematically intercept, track, and collect their users' app activity data—regardless of whether those users turn off "Web & App Activity" in their settings.

9. Google's practices infringe upon consumers' privacy; intentionally deceive consumers; give Google and its employees power to learn intimate details about individuals' lives, interests, and app usage; and make Google a potential target for "one-stop shopping" by any government, private, or criminal actor who wants to undermine individuals' privacy, security, or freedom. Through its pervasive and unlawful communication interceptions and massive data tracking and collection business, Google knows every user's friends, hobbies, political leanings, culinary preferences, cinematic tastes, shopping activity, preferred vacation destinations, romantic involvements, and even the most intimate and potentially embarrassing aspects of the user's app browsing histories and usage—regardless of whether the user accepts Google's illusory offer to keep such activities "private." Indeed, notwithstanding consumers' best efforts, Google has made itself an unaccountable trove of information so detailed and expansive that George Orwell himself could not have imagined it.

10. Google must be held accountable for the harm it has caused to its consumers. And it must be prevented from continuing to engage in the covert and unauthorized data tracking and collection from virtually every American with a mobile phone. Beyond the California Constitution, federal and state privacy laws recognize individuals' reasonable expectations of privacy in confidential communications under these circumstances. Federal and California privacy laws prohibit unauthorized interception, access, and use of the contents in electronic communications. The European courts have also recently found the practices at issue illegal. Likewise, American regulators are beginning to recognize Google's abusive practices for what they are.

11. Plaintiffs are individuals whose mobile app usage was tracked by Google during the period after Google first offered users the ability to turn off "Web & App Activity" tracking and the present (the "Class Period") with his or her "Web & App Activity" turned off. Google's tracking and data collection included detailed browsing history data collected by Google, whereby Google created and monetized user information without those users' consent. Plaintiffs bring federal and

California state law claims on behalf of other similarly-situated Google subscribers in the United States (the "Class") arising from Google's knowing and unauthorized interception, copying, taking, use, and tracking of consumers' internet communications and activity, and its knowing and unauthorized invasion of consumer privacy.

II. THE PARTIES

12. Plaintiff JulieAnna Muniz is an adult domiciled in El Cerrito, California. She had an active Google account during the entire Class Period.

13. Plaintiff Anibal Rodriguez is an adult domiciled in Homestead, Florida. He had an active Google account during the entire Class Period.

14. Defendant Google LLC is a Delaware limited liability company with a principal place of business at what is officially known as The Googleplex, 1600 Amphitheatre Parkway, Mountain View, California 94043. Google LLC regularly conducts business throughout California and in this judicial district. Google LLC is one of the largest technology companies in the world and conducts product development, search, and advertising operations in this district.

15. Defendant Alphabet Inc. is a Delaware corporation, organized and existing under the laws of the State of Delaware, with its principal place of business at what is officially known as The Googleplex, 1600 Amphitheatre Parkway, Mountain View, California 94043-1351. Alphabet is the parent holding company of Google LLC. Alphabet owns all the equity interests in Google LLC.[1]

III. JURISDICTION AND VENUE

16. This Court has personal jurisdiction over Defendants because their principal place of business is in California. Additionally, Defendants are subject to specific personal jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiffs' and the Class' claims occurred in this State.

---

[1] During the 2015 reorganization, certain of Google LLC's business segments were spun off and separated into independent entities under the ownership of Alphabet Inc. At various times during the Class Period, certain of the business segments re-merged with Google LLC under one corporate structure. Accordingly, Alphabet Inc. and Google LLC both have been named as defendants in order to ensure all corporate entities who may be found liable for any portion of the alleged wrongdoing are part of this lawsuit.

17. This Court has subject matter jurisdiction over the federal claims in this action, namely the Federal Wiretap Act, 18 U.S.C. § 2511 (the "Federal Wiretap Act") pursuant to 28 U.S.C. § 1331.

18. This Court has subject matter jurisdiction over this entire action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because this is a class action in which the amount in controversy exceeds $5,000,000, and at least one member of the class is a citizen of a state other than California or Delaware.

19. This Court also has supplemental jurisdiction over the state law claims in this action pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy as those that give rise to the federal claims.

20. Venue is proper in this District because a substantial portion of the events and actions giving rise to the claims in this matter took place in this judicial District. Furthermore, Defendants Alphabet Inc. and Google LLC are headquartered in this District and subject to personal jurisdiction in this District.

21. Intradistrict Assignment. A substantial part of the events and conduct which give rise to the claims herein occurred in Santa Clara County.

IV. FACTUAL ALLEGATIONS

A. Google's Persistent, Covert Collection of Private Consumer Data through Google Analytics

22. Google has collected, and continues to collect, an untold amount of consumer data based on online browsing activity. Over 70% of online websites and publishers on the internet (altogether "Websites") utilize Google's website visitor-tracking product, "Google Analytics." Google Analytics is a "freemium" service Google makes available to Websites that provides data analytics and attribution about the origins of a Website's traffic, demographics, frequency, browsing habits on the Website, and other data about visitors.[2]

[2] Google Analytics is "free" to implement if Websites want general reports with pseudo-anonymous data regarding visitors. To obtain more specific and granular data about visitors, Websites must pay a substantial fee, such as by paying for Google's DV360, Ad Hub, or Google Audience products.

23. To implement Google Analytics, Google requires Websites to embed Google's own custom code into their existing webpage code. When a consumer visits a Website, his or her browser communicates a request to the Website's servers to send the computer script to display the Website. This communication and request for content from the consumer is often referred to as a HTTP GET request, to which the Website's servers respond with the computer code script to display the contents of the Website. The consumer's browser then begins to read Google's custom code along with the Website's own code when loading the Website from the Website's server. Two sets of code are thus automatically run as part of the browser's attempt to load and read the Website pages—the Website's code, which loads the content of the Website requested by the consumer, and Google's embedded code, which does something altogether different.

24. Google's embedded code causes the user's browser to send his or her personal information to Google and its servers in California, such as the user's IP address, the URL address (which identifies the particular page of the Website that is being visited), and other information regarding the user's device and browser. Google's data collection almost always occurs without the user's knowledge, as an automatic response to the consumer's request for information from the Website's server. Google does not require that Websites disclose upfront that Google is collecting the visitors' information regardless of what they do, and as further discussed below, Google does not tell its consumers which websites implement Google Analytics. Other than staying off the internet entirely, there is no effective way for consumers to avoid Google Analytics and its surreptitious tracking.

25. By embedding its tracking code through Google Analytics, Google is able to intercept, track, collect, take, compile, and use more communications that reveal personal and consumer data than any company in the world. Because more than 70% of Websites use Google Analytics, Google is able to track and collect a staggering amount of personal and consumer data online in real time. With virtually every click of the mouse to initiate a consumer's internet request, Google intercepts a signal contemporaneously and sends it to its own servers. Those signals contain consumers' personal viewing information and requests, which Google collects, reads, and organizes based on consumers' prior histories. Google then advances its business

interests by using the personal information obtained through this routine practice of covert interception.

26. Contrary to Google's representations, Google tracks consumers even when consumers select "private mode" on their browsers, including while consumers are "Incognito" on Google Chrome.[3] Google does this through Google Analytics because the Google Analytics tracking code continues to run each time a Website is loaded regardless of whether a user is browsing in "private mode" or not. Thus, unbeknownst to most consumers, Google constantly tracks what they request and read on the internet, click by click and page by page, in real time.

B. Google's Persistent Collection of Mobile App Communications

27. In addition to its unauthorized collection of consumer web data through Google Analytics, Google also engages in the same surreptitious tracking practices with respect to consumer use of mobile apps.

28. Consumers' mobile app usage has grown exponentially in recent years, and Google views this activity as the new frontier in its multi-billion dollar data tracking and collection business. Indeed, Google has already publicly announced that it is prioritizing mobile app results in its search function, and that its search results have preferred mobile app pages over webpages since July 1, 2019.

29. Google tracks consumers' use of mobile apps via a software development kit ("SDK") called Firebase, which Google purchased as part of its acquisition of Firebase, Inc., in 2014. Firebase SDK is a suite of software tools that purports to provide additional functionality to an app, especially if it is to be released for Android. Google acquired Firebase SDK as part of its efforts to "index" the world's mobile apps, which permits Google Search to present search results not just from webpages but also directly from indexed pages within mobile apps. Notably, "Google Search uses information about the actions users take on public and personal content in an app to improve ranking for Search results and suggestions." *Log User Actions*, FIREBASE, https://firebase.google.com/docs/app-indexing/android/log-actions (last visited July 1, 2020).

[3] This specific misconduct is detailed in a separate lawsuit pending in the Northern District of California. *See Brown et al. v. Google LLC et al.*, Case No. 20–cv–03664–LHK (N.D. Cal.).

Google uses Firebase SDK for its own benefit with Google Search by "log[ging] user actions through the App Indexing API." *Id.* Through Firebase SDK, Google can "[l]og the user's interactions with the app, including viewing content, creating new content, or sharing content." *Id.*

30. For example, through Firebase SDK, Google can identify certain "actions" consumers take within an app, such as "viewing a recipe," and then "log separate calls" for each time the consumers "view[] a recipe (start) and then clos[e] the recipe (end)." *Id.*

31. In other words, Google aggressively tracks what consumers browse, see, create, and share online when using the apps installed on their mobile devices.

32. As Search Engine Watch explained in 2015,[4] "Google can index the content contained within an app, either through a sitemap file or through Google's Webmaster Tools. If someone searches for content contained within an app, and if the user has that app installed, the person then has the option to view that content within the app, as opposed to outside the app on a mobile webpage. For sites that have the same content on their main website and app, the app results will appear as deep links[5] within the search listing. If the user has the app installed and they tap on these deep links, the app will launch and take them directly to the content." Firebase SDK enables a number of tracking and data collection functions, including: what the app user is looking at; how the user was guided to launching the application; how the user navigates within the application; what actions the user takes within the application; and whether the app user ultimately pays for a transaction (like booking a hotel) within the application.

33. Firebase SDK automatically collects information from apps, similar to how Google Analytics automatically collects information from online websites. Indeed, as Google itself explains to app developers: Firebase's "[a]utomatically collected events are triggered by basic

---

[4] Christopher Ratcliff, *What Is App Indexing and Why Is It Important?*, SEARCH ENGINE WATCH (Nov. 19, 2015), https://www.searchenginewatch.com/2015/11/19/what-is-app-indexing-and-why-is-it-important/.

[5] Deep links are like hyperlinks to a specific page location within a mobile application.

interactions with your app. As long as you use the Firebase SDK, you don't need to write any additional code to collect these events." These "[a]utomatically collected events" include: (a) "page_location," (b) "page_referrer," and (c) "page_title." Google states that these three parameters are "collected by default with every event."[6] This means that every time the user interacts with an app, Firebase records that interaction by compiling at least those parameters into the user's history.

34. Firebase SDK often does this automatic collection of information in conjunction with Google's older app SDK, called AdMob SDK. Like Firebase SDK, AdMob SDK also automatically collects app-related information.[7] AdMob is owned by Google and is one of the largest mobile advertisement exchanges, and Google required that publishers integrate AdMob SDK in order to use AdMob.

35. Google's tracking of app activity occurs not only in its own apps, which utilize Firebase and AdMob, but also on third-party apps that have no formal association or affiliation with Google other than simply utilizing the Firebase SDK. Those third-party apps utilizing the Firebase SDK include, for example, The New York Times, Duolingo, Alibaba, Lyft, Venmo, Shazam, and The Economist.

36. All consumer requests for content from an app using Firebase SDK are accessible, collectible, trackable, and usable by Google—***regardless*** of whether the user has expressly revoked permission for Google to collect and use such information.

37. Google uses all of this tracked data to enhance its targeted advertising algorithms.

38. When Google collects such information via Firebase, Google intercepts private communications between app users and the app publisher—that is, Google intercepts the app user's request for specific content from the publisher. The communications collected by Firebase

---

[6] *See Automatically Collected Events*, FIREBASE HELP, https://support.google.com/firebase/answer/6317485?hl=en#:~:text=Automatically%20collected%20events%20%20%20%20Event%20name,currency%2C%20quan%20...%20%2023%20more%20rows%20 (last visited June 29, 2020).

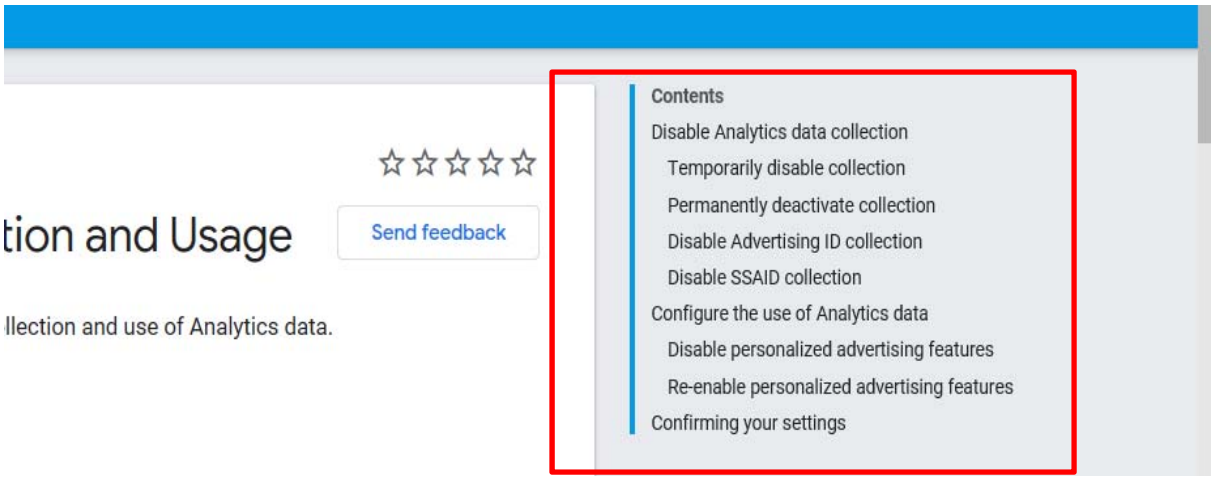
[7] *See Automatically Collected Events*, GOOGLE ADMOB HELP, https://support.google.com/admob/answer/9755157?hl=en (last visited July 1, 2020).

are simultaneously transmitted to Google servers in California, and Google is thereby able to analyze at least what the user is viewing (i.e., the "page_title"), if the user arrived at that page from another place where Google has a tracker (i.e., the "page_referrer"), and the page URL (i.e., the "page_location"). Google then uses the data to target the user with advertisements throughout Google's advertising ecosystem—including in the very app where the communication was intercepted. All consumers' requests for content from the app thereby become accessible, collectible, and usable by Google—regardless of whether the user has expressly revoked permission for Google to collect and use such information.

39. The data collected by Firebase SDK are contemporaneously and automatically sent to Google servers and compiled by Google as part of its profiles on all consumers in the world, access to which Google then sells to advertisers for billions of dollars. Google explains none of this to its users.

40. Publishers often have little choice in whether to use Firebase SDK, because Google requires the use of Firebase in the mobile ecosystem, particularly if publishers want access to Android operating system services, advertisement services, or analytics—all services where Google has market power. Notably, web and app publishers lack control over the information Google can collect from apps using Firebase. If online publishers want to integrate their Google web analytics with mobile app analytics—that is, those publishers that have both websites and apps and want analytics on both—Google *requires* that the publishers integrate Firebase SDK as part of their apps. Because Google Analytics is so widely used, Google's tethering of Google Analytics with Firebase SDK makes Firebase SDK more pervasive, thereby making it even more difficult for consumers to avoid the many tentacles of Google's data and content tracking practices.

41. Once app publishers integrate Firebase SDK as part of their apps, they must play by Google's rules. Google's entire "configuration" menu on its Firebase documentation offers the following limited choices:



Google essentially gives app publishers an all-or-nothing proposition: app publishers must either trust Google with everything Google collects about their users through the app (and that Google will comply with all laws and legal requirements), or publishers must effectively abandon Google's SDK altogether.[8] That app publishers—not to mention consumers and users—can "choose" how Google collects and uses consumer data is an illusion.

42. Since the acquisition of Firebase in 2014, Google has quietly collected what must be the largest index of mobile app pages in the world, with over 1.5 million apps being effectively forced to use Firebase SDK, including most apps on Android OS. Google has also continued to use its monopoly power with respect to web-based searching to push rapid adoption of Firebase SDK, so that it can eventually release a "more complete" Search product that includes every mobile app page in the world. As a result, nearly every Android OS user (and most iOS users) are likely to have fallen victim to Google's deceptive acts.

C. Google's Misrepresentations about Data Privacy

43. Over the last few years, the public, legislators, enforcement agencies, and courts have become increasingly aware of online threats to consumer privacy—including threats posed by powerful technology companies that have become household names. Google has responded by

[8] *See Configure Analytics Data Collection and Useage*, FIREBASE HELP, https://firebase.google.com/docs/analytics/configure-data-collection?platform=android.

telling consumers that they can prevent Google from tracking their online history and collecting their personal data.

44. In Google's Privacy Policy, Google throughout the Class Period made and continues to make numerous assurances about how consumers can "control" the information consumers share with Google, and that they can engage in online activities anonymously and without their communications being intercepted by Google.

45. Google's Privacy Policy explicitly states: "you can adjust your privacy settings ***to control what we collect and how your information is used***." Privacy & Terms, GOOGLE, https://policies.google.com/privacy (emphasis added).

> privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

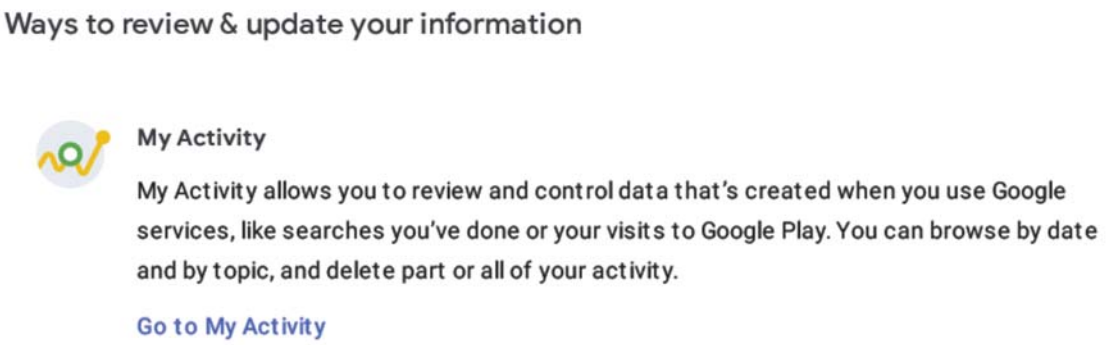
46. Google included this same statement—"you can adjust your privacy settings to control what we collect and how your information is used"—in versions of its Privacy Policy dated May 25, 2018, January 22, 2019, October 15, 2019, December 19, 2019, March 31, 2020, and July 1, 2020. Earlier versions of Google's Privacy Policy included similar representations regarding users' ability to adjust privacy settings and control Google's collection and use of their information.[9]

47. On the "Go to My Activity" page of the Privacy Policy, both in the current version and prior versions published by Google during the Class Period, Google reiterates that "My Activity allows you to review and ***control data that's created when you use Google services***…"

---

[9] For example, the Google Privacy Policies effective between August 19, 2015 and May 24, 2018 included a section titled "Transparency and choice." That section states that Google's "goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used" and directs users to "[r]eview and update your Google activity controls to decide what types of data, such as videos you've watched on YouTube or past searches, you would like saved with your account when you use Google services." Also included in the "Transparency and choice" section is the statement that users can "[c]ontrol who you share information with through your Google Account." *See* Aug. 19, 2015 Google Privacy Policy; Mar. 25, 2016 Google Privacy Policy; June 28, 2016 Google Privacy Policy; Aug. 29, 2016 Google Privacy Policy; Mar. 1, 2017 Google Privacy Policy; Apr. 17, 2017 Google Privacy Policy; Oct. 2, 2017 Google Privacy Policy; Dec. 18, 2017 Google Privacy Policy (this policy was effective until May 24, 2018).

(emphasis added).



48. When consumers click on "Go to My Activity," they are presented with the option to "Learn more." When consumers click on "Learn more," they are taken to a page where they are supposed to be able to "View & control activity in your account."[10]

49. From the "View & control activity in your account" page, a consumer can also click the link, "See & control your Web & App Activity" on the right-hand side.[11] On that page, currently and previously during the Class Period, Google made and makes the following critical representations:

> **See & control your Web & App Activity**
>
> If Web & App Activity is turned on, your searches and activity from ***other Google services*** are saved in your Google Account, so you may get more personalized experiences, like faster searches and more helpful app and content recommendations.
>
> ***You can turn Web & App Activity off or delete past activity at any time.***
>
> …
>
> **What's saved as Web & App Activity**
>
> …

[10] *See View & Control Activity in Your Account*, GOOGLE ACCOUNT HELP, https://support.google.com/accounts/answer/7028918?co=GENIE.Platform%3DDesktop&hl=en#:~:text=View%20%26%20control%20activity%20in%20your%20account%20When,can%20stop%20saving%20most%20activity%20at%20any%20time (last visited June 29, 2020).

[11] *See & Control Your Web & App Activity*, GOOGLE SEARCH HELP, https://support.google.com/websearch/answer/54068?visit_id=637255508625725742210537612 8&hl=en&rd=1 (last visited June 29, 2020).

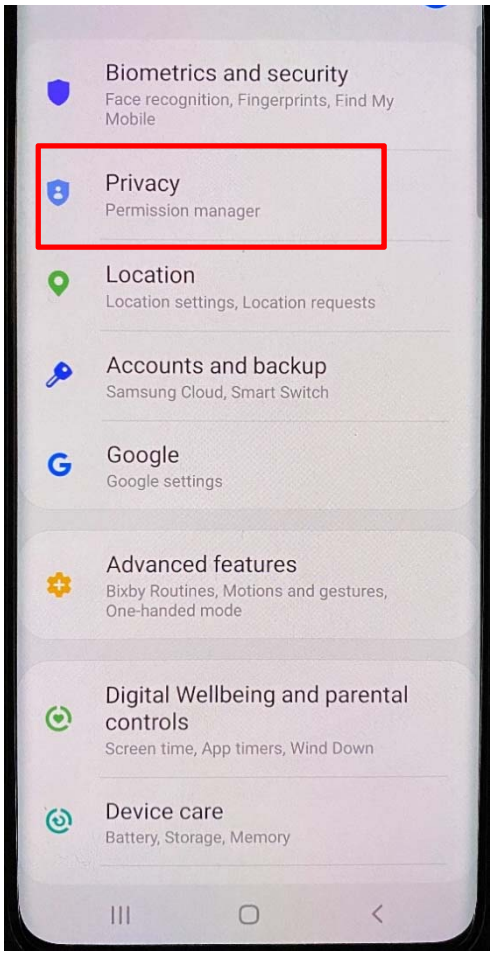
> Info about your browsing and other activity on sites, apps, and devices that use Google services
>
> When Web & App Activity is on, you can include additional activity like:
>
> - Sites and apps that partner with Google to show ads
> - Sites and apps that use Google services, including data that apps share with Google
> - Your Chrome browsing history
> - Android usage & diagnostics, like battery level and system errors
>
> ***To let Google save this information:***
>
> - ***Web & App Activity must be on***.

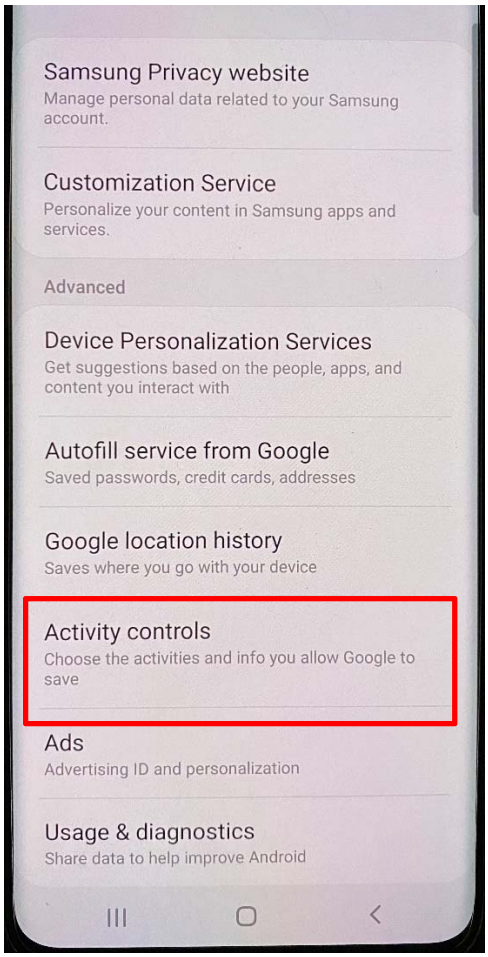
(emphasis added).

50. Google during the Class Period made and continues to make these representations in a Google Help Center webpage titled "See & control your Web & App Activity" on support.google.com. That Google webpage describes how Google collects detailed user information "When Web & App Activity is on" such as "Your location, language, IP address, referrer, and whether you use a browser or an app" and "Information on your device like recent apps or contact names you searched for." In connection with "Info about your browsing and other activity on sites, apps, and devices that use Google services" the webpage again describes Google's data collection "When Web & App Activity is on," but states "To let Google save this information: Web & App Activity must be on."

51. Based on these explicit representations, consumers reviewing Google's Privacy Policy page and "See & control your Web & App Activity" page are left with the reasonable impression that Google will stop collecting *all* of their mobile app information or activity if the "Web & App Activity" setting is turned "off."

52. For consumers who use a mobile phone that employs Google's Android Operating System, Google made and makes similar representations. For example, a Samsung S20 user would see the following screens when they go to "Settings," which then leads the user to a "Privacy Permission Manager":





53. If the user clicks "Activity Controls," the user can purportedly "[c]hoose the activities and info you allow Google to save," and the user is then taken to a web version of Google's online account control, where the user is again purportedly allowed to turn off or on "Web & App Activity":

//

//

//

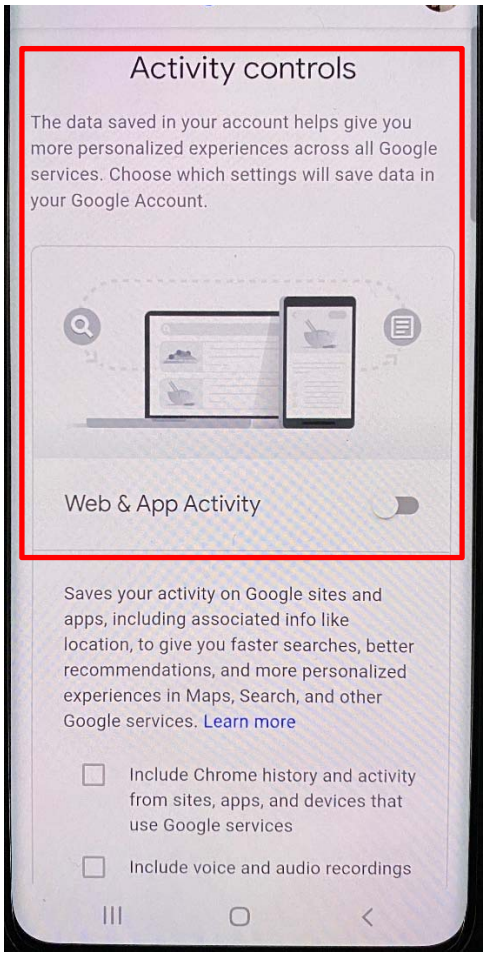
//

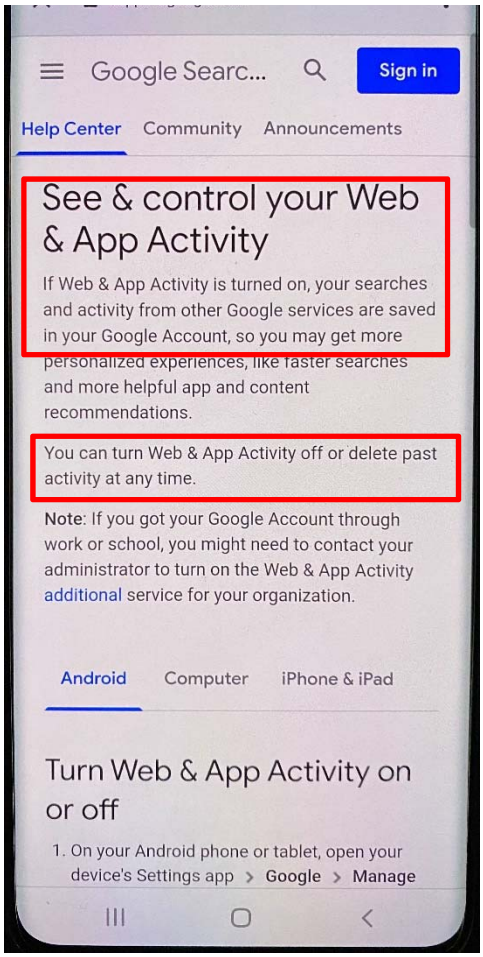
//

//

//

//





54. As can be seen from the mobile version of the "See & Control Your Web & App Activity" page, Google made and makes the same representations to its mobile users as it does to web users—namely:

//

//

//

//

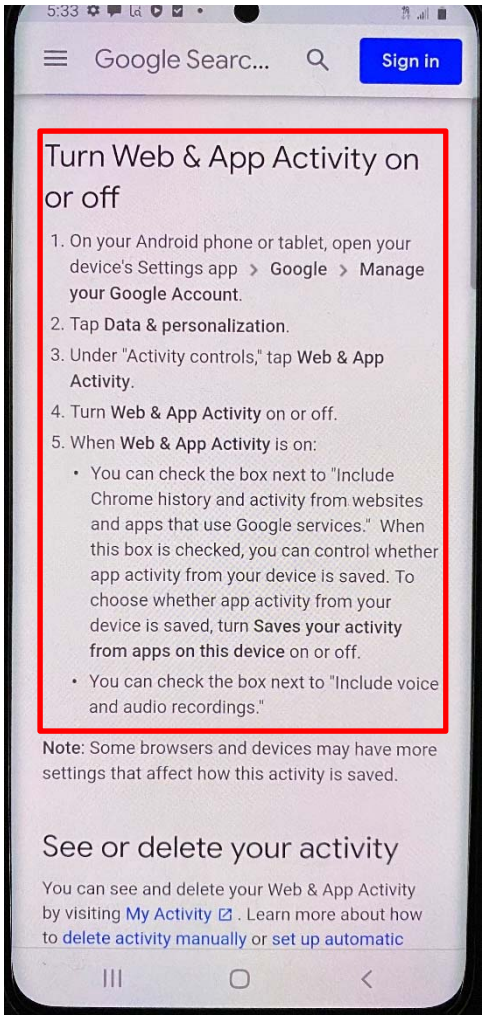
//

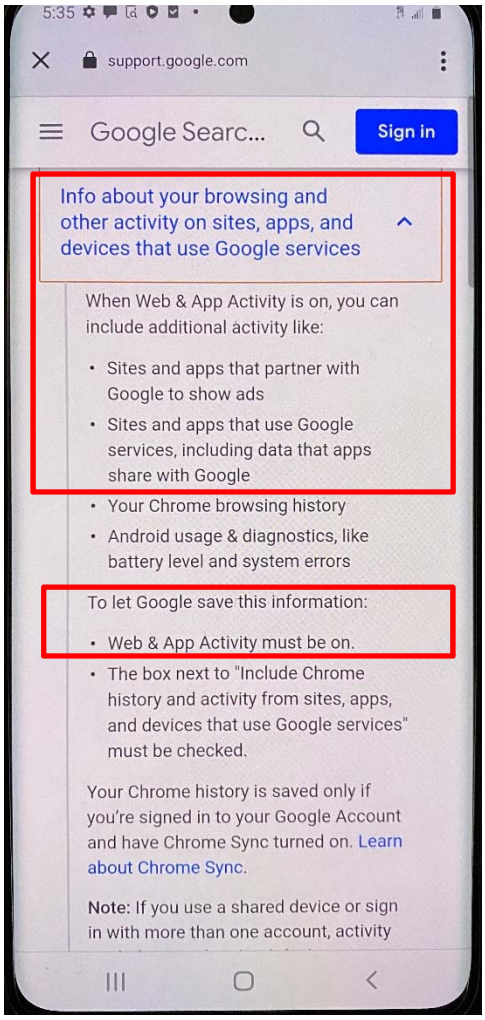
//

//

//

//





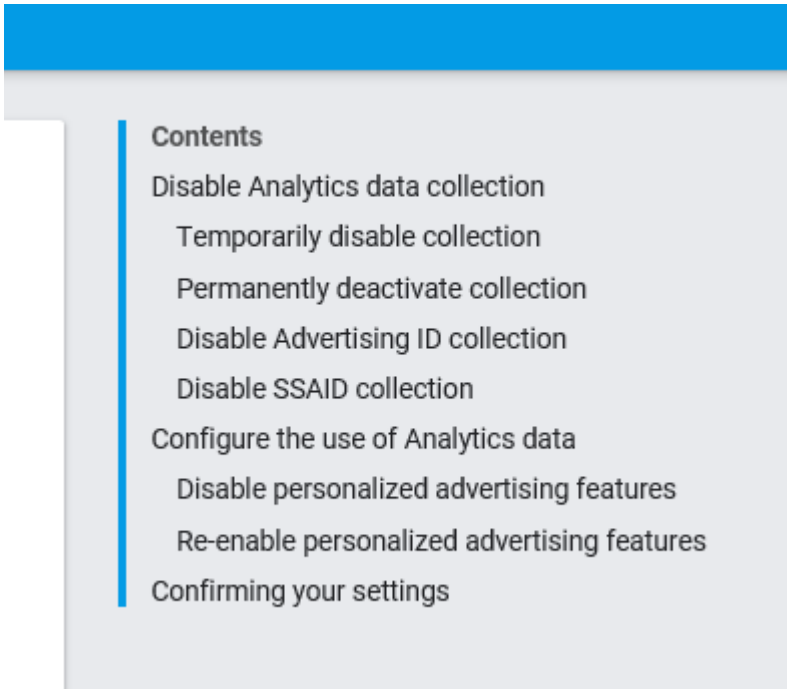
55. Based on these explicit representations, consumers reviewing Google Android OS's Activity Controls are left with the reasonable impression that Google will stop collecting *all* of their mobile app information or activity if the "Web & App Activity" setting is turned "off."

D. Google Continues to Intercept the Communications of Consumers Even When "Web & App Activity" Is Turned Off

56. Google's representations about how it does not track consumers when consumers turn off "Web & App Activity" were and are completely false and misleading. Not only do consumers not know about what Google is doing to collect their private data while they are browsing apps on their devices, based on Google's intentionally false representations, they also have no meaningful way of avoiding Google's data-collection practices, even if they are following Google's instructions to turn off "Web & App Activity."

57. Despite Google's representations that consumers are in control of the private information Google will track and collect, Google's Firebase SDK is actually designed to automatically track consumers and their communications on their mobile apps—***no matter what settings a user chooses***. This is true even when a user browses an app with "Web & App Activity" turned off. Regardless of what a mobile user does, Google automatically collects user communications and events on any app using Firebase SDK. These communications include, at a minimum, the user's (a) "page_location," (b) "page_referrer," and (c) "page_title" in the mobile app, which data further reveals other user identifying information, including, at minimum, the user's device information (which may, for example, include unique identifying information to the device, tagged by Google itself).

58. Again, as demonstrated by Google's own Firebase documentation, there is no setting for app publishers (much less app users) to set Firebase SDK to adhere to user's Google-account-level settings:



59. Although Google intentionally gives its consumers the impression that they have control over whether, how, and when Google collects their personal app data, Google's own documentation shows that Google's privacy guarantees are completely illusory. Google's Firebase

SDK collects personal information and communications content from mobile apps, originating from Google account holders, regardless of their clearly expressed directives to Google and Google's promise to honor those directives.

60. The data Google surreptitiously collects through Firebase SDK is precisely the type of private, personal information consumers wish and expect to protect when they take the steps Google sets out for users to control the private information Google collects. Google knowingly and intentionally tracked, and continues to track, Plaintiffs regardless of Plaintiffs' directives to Google and no matter how sensitive or personal their online app activities are. By accessing Plaintiffs' mobile devices and tracking, collecting, and intercepting Plaintiffs' personal communications—regardless of whether Plaintiffs have attempted to avoid such tracking pursuant to Google's instructions—Google has gained a complete, cradle-to-grave profile of Plaintiffs without their knowledge and contrary to their expressed denial of consent.

61. There is no justification for Google's secret, misleading, and unauthorized interception and collection of consumers' private communications and app activity. Even to the extent Google claims it aggregates this data for later use and sale, this process would occur only *after* Google already intercepted, collected, reviewed, and analyzed individual user information. What Google does with consumers' individual mobile app information after it has secretly intercepted it is cold comfort for those whose privacy Google has already violated, especially because Google repeatedly promises not to engage in this very behavior. By secretly breaking its privacy promises, Google breaches its consumers' expectations of privacy—expectations that Google itself has gone to great lengths to create through its false and lofty pronouncements about its concern for user privacy.

62. The illusion that Google is a good corporate citizen is finally beginning to erode. France's highest court recently affirmed a €50 million fine by the Commission Nationale de l'informatique et des Libertés (CNIL) against Google for its data collection and use practices in connection with Google's Android OS. The CNIL found that Google used "a non-transparent consent gathering process that does not give consumers enough information to make an informed decision and—the bigger issue—the lack of a legal basis for processing personal data for

advertising purposes."[12] In levying this fine, the CNIL stated that its "objective was to verify compliance with IT law and freedoms and the [European Union's General Data Privacy Regulation] of the processing of personal data carried out by GOOGLE, by analyzing the journey of a user and the documents to which he can have access by creating a Google account during the configuration of its mobile equipment under Android." The CNIL found that Google's consent process with Android OS violated the GDPR because there was "a breach of transparency and information obligations" and there was also a "failure to have a legal basis for advertising personalization processing."[13]

63. Similarly, in May 2020, the Arizona Attorney General filed a complaint against Google alleging that Google deceptively tracks consumers and their associated geographical location by making consumers think that they had opted to turn off location tracking through global user-based controls, while making every effort to circumvent such controls. *See* Complaint, *Arizona v. Google LLC,* Arizona Sup. Ct., Case No. 2020-006219 (May 27, 2020). Indeed, the Arizona Attorney General alleges, "Google's deceptive and unfair conduct extends well beyond its false Location History disclosure. Indeed, such acts and practices pervade Google's seemingly relentless drive to (i) collect as much user location data as possible and (ii) make it exceedingly hard for consumers to understand what is going on with their location information." *Id.* ¶ 9. In addition, the Complaint alleges "though Google claims to have obtained consent to collect and store its consumers' data, that consent is based on misleading user interface." *Id.* ¶ 48.

E. Google Intercepts Communications for Its Own Nefarious Purposes, and Not For Those of the Consumer

64. Google represents on its website that "Google was founded on the belief that everything we do should always respect the user." It proclaims a commitment to privacy and

---

[12] Allison Schiff, *Google Loses Its Appeal on 50 Million Euro GDPR Fine*, AD EXCHANGER (June 12, 2020), https://www.adexchanger.com/privacy/google-loses-its-appeal-on-50-million-euro-gdpr-fine/.

[13] *The CNIL's Restricted Panel Announces a Penalty of 50 Million Euros Against Google LLC*, CNIL (Jan. 21, 2019), https://translate.google.com/translate?hl=en&sl=fr&u=https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la&prev=search.

promotes the illusion of user control.

65. What Google does not publicly celebrate, however, is how the company profits from the endless amount of personal and consumer data it secretly intercepts and collects. The more consumer information Google intercepts, analyzes, and collates, the more valuable are the individual consumer profiles that Google creates and sells to third parties for advertising and other uses. This data collection and sale is the centerpiece of Google's business model and the reason Google is pushing for the widespread adoption of Firebase.

66. In a *Wired* article regarding Google's privacy practices, Professor Douglas Schmidt, who has studied Google's user data collection and retention policies for years, stated: Google's "business model is to collect as much data about you as possible and cross-correlate it so they can try to link your online persona with your offline persona. This tracking is just absolutely essential to Google's business. 'Surveillance capitalism' is a perfect phrase for it."[14] By collecting increasing amounts of user data, Google is able to leverage such data to grow its third-party advertising business and profits.

67. Through its spokespersons and in public-facing statements, Google continuously tries to give consumers the false impression that Google is merely acting on behalf of websites and apps as a vendor, or on behalf of consumers to help customize their browsing experience. However, Google does not just serve the interests of consumers or publishers; it also serves itself by using consumer data to generate billions in revenue through its data collection and associated advertising products.

68. In an *NBC News* article regarding Google's endless trove of consumer data, Professor David Yoffie of the Harvard Business School stated, "Google is walking a very fine line. Search, plus Android gives Google amazing insight into individual behavior. Google's stated privacy policies seem adequate, but the question that I cannot answer is whether Google's stated

---

[14] Lily Hay Newman, *The Privacy Battle to Save Google from Itself*, WIRED (Nov. 1, 2018), https://www.wired.com/story/google-privacy-data/.

policy and actual behavior are one and the same."[15] As explained herein, the Google's stated privacy policy and actual behavior are *not* one and the same. Google promises user control and privacy. In practice, Google is a voyeur extraordinaire.

69. Plaintiffs are informed and believe that one of the most telling facts confirming Google's "actual behavior" is that although Google often argues that it is collecting data from publishers and app publishers for their sake, and not for Google's sake, Google often demands significant upgrades (e.g., such as to Google's DV360, a very expensive upgrade) in order for the publishers to see specific visitor information. Otherwise, what the publishers and app publishers believe are their own visitors' information is not available to them except at a general level. That Google possesses, and also holds hostage, such detailed information regarding visitors is proof that Google intercepts and collects consumer information primarily for its own use and financial gain.

70. Plaintiffs are informed and believe that Google also uses the consumer data it collects to iterate on existing Google products and develop new Google products, such as Google's artificial intelligence technology, Google Assistant, which is often on mobile devices. This collection, usage, or monetization of user data contravenes the steps Plaintiffs and Class members have taken to try to control their information from being tracked or used by Google in any way.

V. CONSUMERS REASONABLY EXPECT THAT THEIR PRIVATE COMMUNICATIONS WILL NOT BE INTERCEPTED, COLLECTED, OR MISUSED

71. Plaintiffs and Class members had a reasonable expectation of privacy that when using non-Google branded apps while having opted out of "Web & App Activity" tracking, Google would not intercept, collect, record, disclose, or otherwise misuse their personal communications and data.

72. Plaintiffs' and Class members' expectation of privacy is deeply enshrined in California's Constitution. Article I, section 1 of the California Constitution provides: "All people

[15] Ben Popken, *Google Sells the Future, Powered by Your Personal Data,* NBC NEWS (May 10, 2018), https://www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-n870501.

are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy*."

73. The phrase "*and privacy*" was added in 1972 after voters approved a proposed legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating:

> The right of privacy is the right to be left alone…It prevents government *and business interests* from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.[16]

74. Consistent with the language and intent of Proposition 11, a number of studies examining the collection of consumers' personal data confirm that the surreptitious taking of personal, confidential, and private information—as Google has done and does—violates expectations of privacy that have been established as general social norms. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares a subscriber's personal data. Indeed, a recent study by Consumer Reports shows that 92% of Americans believe that internet companies should be required to obtain consent before selling or sharing their data and the same percentage of Americans believe internet companies should be required to provide consumers with a complete list of the information that has been collected about them.[17]

75. Furthermore, Plaintiffs and Class members had every reason to believe that Google would abide by the representations it made in its "See & control your Web & App Activity"

---

[16] BALLOT PAMP., PROPOSED STATS. & AMENDS. TO CAL. CONST. WITH ARGUMENTS TO VOTERS, GEN. ELECTION *26 (Nov. 7, 1972) (emphasis added).

[17] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds,* CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

controls, and its Android OS "Activity Controls." Again, Android states that "[y]ou can turn Web & App Activity off or delete past activity at any time," and that "[t]o let Google save this information . . . Web & App Activity must be turned on." Google, however, did not abide by its representations to Plaintiffs and Class members, and its conduct of secretly tracking and collecting communications from Plaintiffs' and Class members' private app browsing constitutes a serious invasion of their privacy.

VI. THE VALUE OF INTERCEPTED COMMUNICATIONS

76. Google's continuous interception of consumers' communications and massive consumer-data collection efforts is no accident. Google is one of the largest technology companies in the world. Google LLC and its parent Alphabet Inc. have over 1.5 billion active account consumers, and Alphabet boasts a net worth exceeding $950 billion.

77. Google's enormous financial success results from its unparalleled tracking and collection of consumer personal information and its selling and brokering of that information to optimize advertisement services and generate billions of dollars in revenue for Google.

78. Over the last five years, virtually all of Google's revenue was attributable to third-party advertising, and it is continuously driven to find new and creative ways to leverage its access to consumers' data in order to sustain its phenomenal growth.

79. Google profits from consumers by acquiring their sensitive and valuable personal information, which includes far more than mere demographic information and volunteered personal information like name, birth date, gender and email address. Through its various unauthorized tracking practices, Google plants numerous tracking mechanisms on consumers' devices and apps, which allow Google to track consumers' app browsing histories and correlate them with user, device, and browser IDs.

80. The information Google tracks has and had massive economic value during the Class Period. This value is well understood in the e-commerce industry, and personal information is now viewed as a form of currency.

81. Professor Paul M. Schwartz noted in the Harvard Law Review:

> Personal information is an important currency in the new

> millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056–57 (2004).

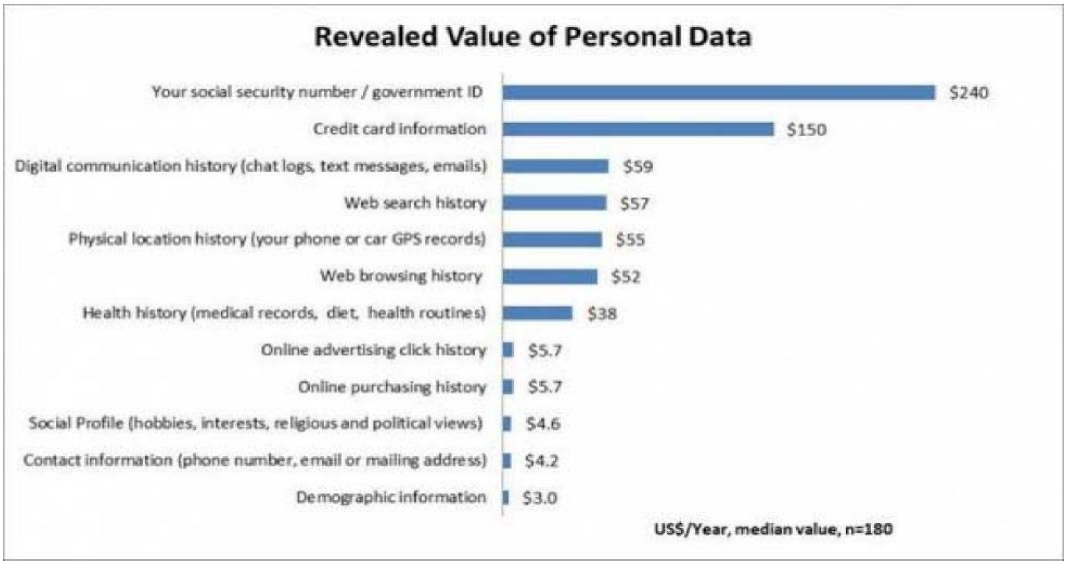
82. Likewise, in the *Wall Street Journal*, former fellow at the Open Society Institute (and current principal technologist at the ACLU) Christopher Soghoian noted:

> The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online.
>
> Although we now regularly trade our most private information for access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.

Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE WALL STREET J. (Nov. 15, 2011), https://www.wsj.com/articles/SB10001424052970204190704577024262567105738.

83. The cash value of consumers' personal information provided during the Class Period to Google as a condition of membership is quantifiable. For example, in a study authored by Tim Morey, as early as 2011, researchers studied the value that 180 internet consumers placed on keeping personal data secure.[18] Contact information of the sort that Google requires was valued by the study participants at approximately $4.20 per year. Demographic information was valued at approximately $3.00 per year. But web browsing histories were valued at a much higher rate: $52.00 per year. The chart below summarizes the findings:

[18] Tim Morey, *What's Your Personal Data Worth?*, DESIGN MIND (Jan. 18, 2011), https://web.archive.org/web/20131206000037/http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html.



84. Similarly, the value of user-correlated internet browsing history is quantifiable, because Google itself was willing to pay consumers for the exact type of communications that Google illegally intercepted from Plaintiffs and Class members during the Class Period. For example, Google had a panel during the Class Period (and still has one today) called "Google Screenwise Trends" which, according to the internet giant, is designed "to learn more about how everyday people use the Internet."

85. Upon becoming a panelist, internet users would add a browser extension that shares with Google the sites they visit and how they use them. The panelists consented to Google tracking such information for three months in exchange for one of a number of "gifts," including gift cards to retailers such as Barnes & Noble, Walmart, and Overstock.com.

86. After three months, Google also agreed to pay panelists additional gift cards "for staying with" the panel. These gift cards, mostly valued at exactly $5, demonstrated conclusively that internet industry participants understood the enormous value in internet users' browsing habits. Today, Google now pays Screenwise panelists up to $3 *per week* to be tracked.

87. As demonstrated above, user-correlated mobile app-page history has monetary value. Google's actions—its unauthorized collection and use of Plaintiffs' and Class members' data—directly caused Plaintiffs' and Class members' data to be sold without permission and to become less valuable. These actions have unjustly enriched Google. Plaintiffs and Class members retain a stake in the profits Google garnered from Plaintiffs' and Class members' personal data,

including without limitation their browsing histories, and it is unjust for Google to retain it.

88. User-correlated mobile app-page history also has non-monetary, privacy value. For example, in a recent study by the Pew Research Center, 93% of Americans said it was "important" for them to be "in control of who can get information" about them. Seventy-four percent said it was "very important." Eighty-seven percent of Americans said it was "important" for them not to have someone watch or listen to them without their permission. Sixty-seven percent said it was "very important." And ninety percent of Americans said it was "important" that they be able to "control[] what information is collected about [them]." Sixty-five percent said it was very important.

89. Likewise, in a 2011 Harris Poll study, seventy-six percent of Americans agreed that "online companies, such as Google…control too much of our personal information and know too much about our browsing habits." Public opinion has only become increasingly adverse to Google's monopoly power over consumer data.

VII. TOLLING OF THE STATUTE OF LIMITATIONS

90. The applicable statutes of limitations have been tolled by Google's knowing and active concealment and denial of the facts alleged herein.

91. Google has repeatedly represented that its users could prevent Google from tracking user app viewing history and activity data by turning off "Web & App Activity" from their Google accounts, or from Android OS "Account Controls." Nowhere did Google ever represent that it would continue to track user data once these steps were performed, nor has Google ever disclosed that it will still attempt to collect, aggregate, and analyze user data so that it can continue to track individual consumers even when the user has followed Google's instructions on how to use mobile apps privately.

92. Accordingly, Plaintiffs and the Class could not have reasonably discovered the truth about Google's practices until shortly before this class litigation was commenced. Plaintiffs only learned of the truth in the weeks leading up to the filing of this Complaint.

//

//

VIII. PLAINTIFF-SPECIFIC FACTUAL ALLEGATIONS

93. Plaintiff JulieAnna Muniz is an adult domiciled in California and has an active Google account and had an active account during the entire proposed Class Period.

94. She accessed the Internet through various apps supported by Firebase SDK, including but not limited to Shazam and Lyft. She sent and received communications through these apps on mobile devices which were computing devices that were not shared devices.

95. At various times in 2020, she accessed numerous app pages (such as those in Shazam and Lyft) containing content she was interested in, on her Apple device while "Web & App Activity" was turned off. Her communications with the app were nevertheless intercepted and tracked by Google without her knowledge or consent, on applications such as Shazam and Lyft, which she uses.

96. Plaintiff Anibal Rodriguez is an adult domiciled in Florida and has an active Google account and had an active account during the entire proposed Class Period.

97. He accessed the Internet through various apps supported by Firebase SDK, including but not limited to Lyft and Alibaba. He sent and received communications through these apps on mobile devices which were computing devices that were not shared devices.

98. At various times between at least 2019 and 2020, he accessed numerous app pages (such as those in Lyft and Alibaba) containing content he was interested in on his Android device while "Web & App Activity" was turned off. His communications with the app were nevertheless intercepted and tracked by Google without his knowledge or consent.

99. None of the Plaintiffs consented to the interception of their confidential communications made while their settings are turned "off" for "Web & App Activity" tracking.

IX. CLASS ACTION ALLEGATIONS

100. This is a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure on behalf of the following Classes and Subclasses:

- Class 1 – All individuals who during the Class Period (a) turned off "Web & App Activity," and (b) whose mobile app activity was still tracked by Google via Firebase SDK through a non-Google branded mobile app, (c) on an Android OS mobile device.

- Class 2 – All individuals who during the Class Period (a) turned off "Web & App Activity," and (b) whose mobile app activity was still tracked by Google via Firebase SDK through a non-Google branded mobile app, (c) on any non-Android OS mobile device.

101. Excluded from the Class are: (1) the Court (including any Judge or Magistrate presiding over this action and any members of their families); (2) Defendants, its subsidiaries, parents, predecessors, successors and assigns, including any entity in which any of them have a controlling interest and its officers, directors, employees, affiliates, legal representatives; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel, Class counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

102. **Ascertainability**: Membership of the Class is defined based on objective criteria and individual members will be identifiable from Defendants' records, including from Google's massive data storage, consumer accounts, and enterprise services. Based on information readily accessible to it, Google can identify members of the Class who own an Android device or have a non-Android device who were victims of Google's impermissible interception, receipt, or tracking of communications as alleged herein.

103. **Numerosity**: The Class likely consists of millions of individuals. Accordingly, members of the Class are so numerous that joinder of all members is impracticable. Class members can be identified from Defendants' records, including from Google's consumer accounts and enterprise services.

104. **Predominant Common Questions**: Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Common questions for the Class include, but are not limited to, the following:

a. Whether Google represented that the Class could control what communications of user information, app browsing history, and app activity data were intercepted, received, or collected by Google;

b. Whether Google gave the Class a reasonable expectation of privacy that their

communications of user information, app browsing history, and app activity data were not being intercepted, received, or collected by Google while "Web & App Activity" was turned off;

c. Whether Google in fact intercepted, received, or collected communications of user information, app browsing history, and app activity from the Class while "Web & App Activity" was turned off;

d. Whether Google's practice of intercepting, receiving, or collecting communications of user information, app browsing history, and app activity violated state and federal privacy laws;

e. Whether Google's practice of intercepting, receiving, or collecting communications of user information, app browsing history, and app activity violated state and federal anti-wiretapping laws;

f. Whether Google's practice of intercepting, receiving, or collecting communications of user information, app browsing history, and app activity violated any other state and federal laws;

g. Whether Plaintiffs and the Class are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

h. Whether Plaintiffs and the Class have sustained damages as a result of Google's conduct, and if so, what is the appropriate measure of damages or restitution.

105. **Typicality**: Plaintiffs' claims are typical of the claims of other Class members, as all members of the Class were uniformly affected by Google's wrongful conduct in violation of federal and state law as complained of herein.

106. **Adequacy**: Plaintiffs will fairly and adequately protect the interests of the members of the Class and have retained counsel that is competent and experienced in class action litigation, including nationwide class actions and privacy violations. Plaintiffs and their counsel have no interest that is in conflict with, or otherwise antagonistic to the interests of the other Class members. Plaintiffs and their counsel are committed to vigorously prosecuting this action on

behalf of the members of the Class, and they have the resources to do so.

107. **Superiority**: A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single, able court. Furthermore, as the damages individual Class members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

108. **California Law Applies to the Entire Class**: California's substantive laws apply to every member of the Class, regardless of where in the United States the Class member resides. Defendants' own Terms of Service explicitly states "California law will govern all disputes arising out of or relating to these terms, service specific additional terms, or any related services, regardless of conflict of laws rules. These disputes will be resolved exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts." By choosing California law for the resolution of disputes covered by its Terms of Service, Google concedes that it is appropriate for this Court to apply California law to the instant dispute. Further, California's substantive laws may be constitutionally applied to the claims of Plaintiffs and the Class under the Due Process Clause, *see* U.S. CONST. amend. XIV, § 1, and the Full Faith and Credit Clause, *see* U.S. CONST. art. IV, § 1, of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by the Plaintiffs and all Class members, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair. Defendants' decision to reside in California and avail itself of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims herein constitutionally permissible. The application of California laws to the Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiffs and the proposed Class, and California has a greatest interest in applying its laws here.

109. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

X. COUNTS

COUNT I

VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. § 2510, *ET. SEQ.*

110. Plaintiffs hereby incorporate paragraphs 1 to 109 as if fully stated herein.

111. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

112. The Federal Wiretap Act protects both the sending and receipt of communications.

113. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

114. Google's actions in intercepting and tracking user app communications while Plaintiffs turned off "Web & App Activity" were intentional. On information and belief, Google is aware that it is intercepting communications in these circumstances and has taken no remedial action.

115. Google's interception of communications that the Plaintiffs were sending and receiving while browsing their mobile apps was done contemporaneously with the Plaintiffs' sending and receipt of those communications. In fact, Google received the communications before the communication between the Plaintiffs and the various apps were completed.

116. The communications intercepted by Google included "contents" of electronic communications made from the Plaintiffs to apps other than Google in the form of detailed URL requests, app browsing histories, and search queries which Plaintiffs sent to those apps and for which Plaintiffs received communications in return from those apps.

117. The transmission of data between Plaintiffs and apps on which Google tracked and intercepted Plaintiffs' communications without authorization while "Web & App Activity" was turned off were "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature

transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

118. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The Firebase SDK, computer codes, and programs Google used to intercept and track Plaintiffs' communications while "Web & App Activity" was turned off;

b. Plaintiffs' mobile applications;

c. Plaintiffs' mobile devices;

d. The apps from which Google tracked and intercepted Plaintiffs' communications while "Web & App Activity" was turned off;

e. The Firebase SDK, computer codes and programs used by Google to effectuate its tracking and interception of Plaintiffs' communications while using an app while "Web & App Activity" was turned off; and

f. The plan Google carried out to effectuate its tracking and interception of Plaintiffs' communications while using an app while "Web & App Activity" was turned off.

119. Google was not an authorized party to the communication because Plaintiffs were unaware of Google's collection of page locations, page referrers, page titles, and user information, did not knowingly send any of the communication to Google, and were browsing apps while "Web & App Activity" was turned off when Google intercepted the communications between Plaintiffs and apps other than Google. Google could not manufacture its own status as a party to Plaintiffs' communications with others by surreptitiously redirecting or intercepting those communications

120. As illustrated herein, "the" communications between Plaintiffs and apps were simultaneous to, but *separate* from, the channel through which Google illegally acquired the contents of those communications.

121. Plaintiffs did not consent to Google's continued interception of the user's communications after turning off "Web & App Activity" and thus never consented to Google's

interception of their communications. Indeed, Google represented to Plaintiffs and the public that consumers could "control . . . what information [they] share with Google" including with "[p]roducts that are integrated into third-party apps and sites by turning off "Web & App Activity." Moreover, the communications intercepted by Google were plainly confidential, which is evidenced by the fact that Plaintiffs turned off "Web & App Activity" in a manner consistent with Google's own recommendations to prevent sharing of information with Google prior to accessing or communicating with apps.

122. After intercepting the communications, Google then used the contents of the communications knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

123. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiffs and the Class members; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Google in the future, and a reasonable attorneys' fee and other litigation costs reasonably incurred.

COUNT II

VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA")
CALIFORNIA PENAL CODE §§ 631 AND 632

124. Plaintiffs hereby incorporate paragraphs 1 to 109 as if fully stated herein.

125. The California Invasion of Privacy Act is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

126. Cal. Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars . . . .

127. Cal. Penal Code § 632(a) provides, in pertinent part:

> A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars . . . .

128. Under either section of the CIPA, a defendant must show it had the consent of all parties to a communication.

129. Google has its principal place of business in California; designed, contrived and effectuated its scheme to track and intercept consumer communications while they were browsing apps from their device while "Web & App Activity" was turned off; and has adopted California substantive law to govern its relationship with its users.

130. At all relevant times, Google's tracking and interceptions of Plaintiffs' communications while using an app with "Web & App Activity" turned off was without authorization and consent from the Plaintiffs.

131. Google's non-consensual tracking of Plaintiffs' communications while using an app with "Web & App Activity" turned off was designed to attempt to learn at least some meaning of the content in the mobile app pages.

132. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Google's deliberate and admittedly purposeful scheme

that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

a. The Firebase SDK, computer codes and programs Google used to track Plaintiffs' communications while "Web & App Activity" was turned off;

b. Plaintiffs' mobile applications;

c. Plaintiffs' mobile devices;

d. The apps from which Google tracked and intercepted Plaintiffs' communications while they were using an app with "Web & App Activity" turned off;

e. The Firebase SDK, computer codes and programs used by Google to effectuate its tracking and interception of Plaintiffs' communications while using an app with "Web & App Activity" turned off; and

f. The plan Google carried out to effectuate its tracking and interception of Plaintiffs' communications while using an app while "Web & App Activity" was turned off.

133. Plaintiffs have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their personally identifiable information.

134. Pursuant to California Penal Code § 637.2, Plaintiffs have been injured by the violations of California Penal Code §§ 631 and 632, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

COUNT III

INVASION OF PRIVACY

135. Plaintiffs hereby incorporate paragraphs 1 to 109 as if fully stated herein.

136. The right to privacy in California's constitution creates a right of action against private entities such as Google.

137. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Google.

138. To plead a California constitutional privacy claim, a plaintiff must show an

invasion of (1) a legally protected privacy interest; (2) where the plaintiff had a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy.

139. As described herein, Google has intruded upon the following legally protected privacy interests:

a. The Federal Wiretap Act as alleged herein;

b. The California Wiretap Act as alleged herein;

c. A Fourth Amendment right to privacy contained on personal computing devices, including web-browsing history, as explained by the United States Supreme Court in the unanimous decision of *Riley v. California*;

d. The California Comprehensive Computer Data Access and Fraud Act, Cal Pen. Code § 502, which applies to Plaintiffs and all Class members by virtue of Google's choice of California law to govern its relationship with Google users;

e. The California Constitution, which guarantees Californians the right to privacy;

f. Google's Privacy Policy and policies referenced therein, and other public promises it made not to track or intercept Plaintiffs' communications or access their computing devices and apps while "Web & App Activity" is turned off.

140. Plaintiffs had a reasonable expectation of privacy under the circumstances in that Plaintiffs could not reasonably expect Google would commit acts in violation of federal and state civil and criminal laws; and Google affirmatively promised consumers it would not track their communications or access their computing devices or apps while they were using an app while in "Web & App activity" was turned off.

141. Google's actions constituted a serious invasion of privacy in that it:

a. Invaded a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices, including

user data, app activity and app browsing histories;

b. Violated several federal criminal laws, including the Federal Wiretap Act;

c. Violated dozens of state criminal laws on wiretapping and invasion of privacy, including the California Invasion of Privacy Act;

d. Invaded the privacy rights of millions of Americans without their consent; and

e. Constituted the unauthorized taking of valuable information from millions of Americans through deceit.

142. Committing criminal acts against millions of Americans constitutes an egregious breach of social norms that is highly offensive.

143. The surreptitious and unauthorized tracking of the internet communications of millions of Americans, particularly where, as here, they have taken active (and recommended) measures to ensure their privacy, constitutes an egregious breach of social norms that is highly offensive.

144. Google's intentional intrusion into Plaintiffs' internet communications and their computing devices and apps was highly offensive to a reasonable person in that Google violated federal and state criminal and civil laws designed to protect individual privacy and against theft.

145. The taking of personally identifiable information from millions of Americans through deceit is highly offensive behavior.

146. Secret monitoring of private app browsing is highly offensive behavior.

147. Wiretapping and surreptitious recording of communications is highly offensive behavior.

148. Google lacked a legitimate business interest in tracking consumers while use an app while "Web & App Activity" was turned off, without their consent.

149. Plaintiffs and the Class members have been damaged by Google's invasion of their privacy and are entitled to just compensation and injunctive relief.

COUNT IV

VIOLATIONS OF CALIFORNIA PENAL CODE § 502
THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA")

150. Plaintiffs incorporate paragraphs 1 to 109 as though set forth herein.

151. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction." Smart phone devices with the capability of downloading and using apps are "computers" within the meaning of the statute.

152. Google violated Cal. Penal Code § 502(c)(2) by knowingly accessing and without permission taking, copying, and using data concerning Plaintiffs' app usage and other personally identifiable information. When Plaintiffs browsed apps with "Web & App Activity" turned off, Google nevertheless knowingly accessed their computing devices. Google then took, copied, and thereafter used personal data from the computing devices without permission, such as user data, app activity, and app browsing history. In fact, Plaintiffs had expressly communicated to Google that Google did not have permission to take, copy, or make use of such data.

153. Accordingly, despite Google's false guarantees to the contrary, Google effectively charged Plaintiffs and other consumers, and profited from them, by acquiring their sensitive and valuable personal information without their permission and using it for Google's own financial benefit to advance its advertising business. Google was thereby unjustly enriched.

154. Google accessed, copied, took, and used data from Plaintiffs' computers in and from the State of California, where Google (1) has its principal place of business and (2) used servers that provided services and communication links between Plaintiffs and Google and other apps, which allowed Google to access user data. Accordingly, Google caused the access of Plaintiffs' computers from California, and is therefore deemed to have accessed the computer in California.

155. As a direct and proximate result of Google's unlawful conduct within the meaning of Cal. Penal Code § 502, Google has caused loss to Plaintiffs and has been unjustly enriched in an amount to be proven at trial.

156. Plaintiffs seek compensatory damages and/or disgorgement in an amount to be proven at trial, and declarative, injunctive, or other equitable relief.

157. Plaintiffs are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Google's violations were willful and, upon information and belief, Google is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

158. Plaintiffs and the Class members are also entitled to recover their reasonable attorneys' fees pursuant to Cal. Penal Code § 502(e).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify this action is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Award compensatory damages, including statutory damages where available, to Plaintiffs against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Order Defendants to disgorge revenues and profits wrongfully obtained;

D. Permanently restrain Defendants, and their officers, agents, servants, employees and attorneys, from intercepting, tracking, or collecting communications while Plaintiffs have "Web & App Activity" turned off;

E. Award Plaintiffs their reasonable costs and expenses incurred in this action, including counsel fees and expert fees;

F. Award Plaintiffs punitive or exemplary damages; and

G. Grant Plaintiffs such further relief as the Court deems appropriate.

//

//

//

XI. JURY TRIAL DEMAND

Plaintiffs demand a trial by jury of all issues so triable.

Dated: July 14, 2020

BOIES SCHILLER FLEXNER LLP

/s/ *Mark C. Mao*

Mark C. Mao, CA Bar No. 236165
Beko Reblitz-Richardson, CA Bar No. 238027
Alexander J. Konik, CA Bar No. 299291
BOIES SCHILLER FLEXNER LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
Fax: (415) 293-6899
mmao@bsfllp.com
brichardson@bsfllp.com
akonik@bsfllp.com

James Lee (*pro hac* admission pending)
Rossana Baeza (*pro hac* admission pending)
BOIES SCHILLER FLEXNER LLP
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
Fax: (303) 539-1307
jlee@bsfllp.com
rbaeza@bsfllp.com

Jesse Panuccio (*pro hac* admission pending)
BOIES SCHILLER FLEXNER LLP
1401 New York Ave, NW
Washington, DC 20005
Tel.: (202) 237-2727
Fax: (202) 237-6131
jpanuccio@bsfllp.com

Attorneys for Plaintiffs